UNITED STATES DISTRICT COURT

for the

Western District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

HP PAVILION LAPTOP COMPUTER, SN 5CD3367NVV6

Case No. 6:16MJ1

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Western District of Virginia
(identify the person or describe the property to be searched and give its location):

HP PAVILION LAPTOP COMPUTER, SN 5CD3367NVV6 - Currently in the custody of the Lynchburg Police Department Evidence Vault

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B, (copy attached), herein incorporated by reference.

YOU ARE COMMANDED to execute this warrant on or before March 11, 2016 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Robert S. Ballou.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: Feb 26, 2016 12:35 p.m.

Judge's signature

City and state: Roanoke, VA

Robert S. Ballou, U.S. Magistrate
Printed name and title

Return

Case No.: 6:16MJ1	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

UNITED STATES DISTRICT COURT

for the

Western District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

HP PAVILION LAPTOP COMPUTER, SN 5CD3367NVV6

Case No. 6:16MJ1

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

HP PAVILION LAPTOP COMPUTER, SN 5CD3367NVV6 - Currently in the custody of the Lynchburg Police Department Evidence Vault

located in the Western District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18, USC, Section 875 (C)	Interstate Communication
18, USC, Section 871	Threats Against the President
~~18, USC, Section 879~~	~~Threats Against A Former President~~ 1752

The application is based on these facts:

☑ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Thomas W. Fleming, Senior Resident Agent USSS
Printed name and title

Sworn to before me and signed in my presence.

Date: Feb. 26, 2016

Judge's signature

City and state: Ronaoke, VA

Robert S. Ballou, U.S. Magistrate Judge
Printed name and title

THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF VIRGINIA LYNCHBURG DIVISION

IN THE MATTER OF A SEARCH WARRANT FOR A HP PAVILION LAPTOP COMPUTER, SN 5CD3367NVV6	CASE NO. 6:16MJ1

A F F I D A V I T

I, Thomas W. Fleming, Senior Resident Agent of the U. S. Secret Service (USSS), Roanoke Resident Agency, being duly sworn, depose, and state:

1. I am a duly sworn Special Agent of the USSS, having been so employed since March of 1997 and having been in law enforcement since September 1989. My investigative duties focus primarily on conducting criminal investigations involving counterfeiting of U. S. currency, forgery, bank fraud, false loan applications, wire fraud, credit card fraud, false identification, other financial crime investigations, and protective intelligence/threat investigations.

2. This affidavit is based upon information known to me or received during my investigation, from other law enforcement agencies, and investigative techniques. This

2/26/2016

investigation is being conducted with members of the Veterans Affairs Office of Inspector General (VA OIG), Mid-Atlantic Field Office, who had initiated the investigation, and the Lynchburg Police Department (LPD). Furthermore, the facts and circumstances of this investigation have been summarized for the specific purposes of this application. No attempt has been made to set forth the complete factual history of this investigation or all of its details. In making this application, I am relying only on the facts stated herein.

3. This Affidavit is made in support of an application for a warrant to search and seize property described in Attachment A and Attachment B. The purpose of this application is to seize evidence of a violation of 18 U.S.C. § 875(c) (Interstate Communications), where whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or injure the person of another shall be fined under this title or imprisoned not more than five years or both.

Based upon the investigation detailed below, I submit that evidence, fruits, and instrumentalities of violations of the above-listed statute are located on and/or stored in

RSB 2/26/2016

the property described in Attachment A.

The Investigation

1. On February 15, 2016, the suspect, Karsten Jeffrey SHEPHERD, a veteran of the U.S. Air Force, transmitted via the internet an electronic message (email), an invitation request through the online social networking database, LinkedIn, to the personal electronic message (email) account of "Victim One," who is an executive with VA. According to a screenshot image that was provided to VA OIG, this request was sent from "Karsten Shepherd, C.I.A. Special Access Program, Lynchburg, Virginia." In this request, SHEPHERD asked Victim One to add SHEPHERD to Victim One's LinkedIn network. As part of this request, there was a typed message which read, "Id personally like to kill the whole VA leadership by dismemberment for what you did to me and my family but I have an army coming let the VA leadership know I will get you all killed. The illuminati waged war on the beast. 666."

2. Also included in this February 15, 2016 electronic message (email) LinkedIn invitation request to Victim One was a picture of a white male wearing a backwards hat, white

2/26/2016

long-sleeve t-shirt and silver/metal chain with cross. The individual in this picture has been identified by Lynchburg Police and other federal law enforcement as the suspect, Karsten SHEPHERD. The publicly-available online profile for Karsten SHEPHERD on LinkedIn includes statements about the CIA, Illuminati and Masons. The publicly available online LinkedIn profile for Karsten SHEPHERD also states, ". . . only by God's grace have I not killed someone. . . ."

3. On February 16, 2016, officer(s) of the Lynchburg Police Department conducted a health and welfare check at the residence of SHEPHERD's father located in the City of Lynchburg. According to responding officers, SHEPHERD was located at this residence sitting at the dining room table after being let into the residence by SHEPHERD's father. A responding officer indicated that SHEPHERD was immediately detained since a laptop computer was next to SHEPHERD. The responding officer then indicated that SHEPHERD immediately told his father to shut down the computer and log SHEPHERD off. SHEPHERD's father told the responding officer that the computer belonged to SHEPHERD's father, but SHEPHERD had been using it. The responding officer indicated that SHEPHERD's father gave consent to have the computer seized

2/26/2016

as evidence. The Lynchburg Police Department seized the computer as evidence a "HP Pavilion Laptop Serial #5CD3367NVV6" computer from SHEPHERD's father's residence on this date. The responding officer indicated that SHEPHERD proceeded to tell him that SHEPHERD was part of a secret CIA special access program that had him tortured and he was subjected to watching others being tortured. SHEPHERD told the responding officer that SHEPHERD had everything figured out about the Masons and Illuminati. SHEPHERD also told the responding officer that SHEPHERD had been subjected to constant assassination attempts because of what he knows. SHEPHERD then told the responding officer that SHEPHERD had post-traumatic stress disorder and he was supposed to take medication for anxiety and several other mental health issues, but he was not currently taking his medication. After speaking with SHEPHERD, the officers determined that an Emergency Custody Order (ECO) was appropriate in this instance.

4. On February 16, 2016, officer(s) of the Lynchburg Police Department transported SHEPHERD to Lynchburg General Hospital in accordance with an ECO. A responding officer, who assisted in transporting SHEPHERD indicated that he was present and clearly heard SHEPHERD tell the doctor at

2/26/2016

Lynchburg General Hospital that SHEPHERD had been falsely accused and detained several times in the past; however, this time SHEPHERD deserved it. The responding officer heard SHEPHERD tell the doctor that SHEPHERD had sent several emails that day threatening to kill people. The responding officer then heard SHEPHERD say that he was not actually going to kill these people, but SHEPHERD was going to have other people kill them.

5. The computer seized pursuant to plain view and consent was inventoried and stored as evidence in the LPD property room. The computer remains in property and has not been examined.

6. SHEPHERD's father has subsequently confirmed to federal law enforcement that SHEPHERD was located in Lynchburg, Virginia on February 15, 2016 and had been since the evening of February 8, 2016. SHEPHERD's father also confirmed that SHEPHERD was using LinkedIn on SHEPHERD's father's computer in and around this time. SHEPHERD's father also reported that he visited his son in December 2015 and his son used his father's computer to check his email account. SHEPHERD's father reported that his son never logged out of the account and he has seen email messages from LinkedIn.

7. SHEPHERD has made LinkedIn request to at least one U.S. Secret Service agent on or about February 10, 2016 and notified him of his travels to Washington, DC and has contacted at least one Lynchburg PD officer (ALSO USING LINKEDIN? OR EMAIL??).

8. Victim One received the electronic message (email) invitation request on his "gmail" email account. Preliminary investigation has revealed that gmail is operated by Google, which has no data centers located within the Commonwealth of Virginia.

9. SHEPHRED has had previous contact with the U.S. Secret Service where on or about February 19, 2015 he placed a call to the USSS where he threatened to "knock the President out". On March 20, 2015, he mailed a rambling letter to the White House and on May 13, 2015, he mailed a letter where he threatened to dismember President Obama.

10. On February 9, 2016, SHEPHERD was interviewed by this affiant and he described traveling to multiple state capitals to deliver letters to various government officials.

In addition to the statements of SHEPHERD's father that SHEPHERD used the subject computer to access his LinkedIn account and send emails, based on my experience conducting criminal

2/24/2016

investigations and protective intelligence investigations, I have found that suspects use computers to communicate and conduct research via the internet to further their cause. It is based on this experience that I believe the computer seized may contain information relevant to the investigation as describe in Attachment B.

PROPOSED SEARCH OF THE COMPUTERS

I respectfully submit that there is probable cause to believe that the item identified in the Application and Attachment A contains evidence, contraband, fruits and instrumentalities pertaining to violations 18 U.S.C. § 875 (C) (Interstate Communication), 871 (Threats to the President), 879 (Threats to Former Presidents) among other possible federal offenses. I therefore respectfully request that the attached search warrant be issued authorizing the search of property described in Attachment B.

As explained below the subject computer, will be searched. Computer hardware is used to save copies of files and communications, while printers are used to make paper copies of same. Programs loaded on the drives are the means by which the computer can send, print and save those files and communications. Finally, password and security devices are often used to restrict access to or hide computer software,

RSB 2/26/2016

documentation or data. Each of these parts of the computer is thus integrated into the entire operation of a computer. In order to best evaluate the evidence, the computers—and all of the related computer equipment described above—should be available to a computer investigator/analyst.

1. ***Forensic Analysis.*** After obtaining a forensic image, the data will be analyzed. Analysis of the data following the creation of the forensic image is a highly technical process that requires specific expertise, equipment and software. There are literally thousands of different hardware items and software programs that can be commercially purchased, installed and custom-configured on a user's computer system. Computers are easily customized by their users. Even apparently identical computers in an office environment can be significantly different with respect to configuration, including permissions and access rights, passwords, data storage and security. It is not unusual for a computer forensic examiner to have to obtain specialized hardware or software, and train with it, in order to view and analyze imaged data.

2. Analyzing the contents of a computer, in addition to requiring special technical skills, equipment and software, also can be very tedious. It can take days to properly search a single hard drive for specific data. Searching by keywords, for

RSB 2/26/2016

example, often yields many thousands of "hits," each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. The computer may have stored information about the data at issue: who created it; when it was created; when it was last accessed; when it was last modified; when was it last printed; and when it was deleted. Operation of the computer by non-forensic technicians effectively destroys this and other trace evidence.

3. Moreover, certain file formats do not lend themselves to keyword searches. Keywords search for information in text format. Many common electronic mail, database and spreadsheet applications do not store data as searchable text. The contents of Adobe ".pdf" files are not searchable via keyword searches. The data is saved in a proprietary non-text format. Microsoft Outlook data is an example of a commonly used email program that stores data in a non-textual, proprietary manner-ordinary keyword searches will not reach this data. Documents printed by the computer, even if the document never was saved to the hard drive, are recoverable by forensic examiners, yet they are not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text.

2/26/2016

Similarly, faxes sent to the computer are stored as graphic images and not as text.

4. Analyzing data on-site has become increasingly impossible as the volume of data stored on a typical computer system has become mind-boggling. For example, a single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. A single Terabyte of storage space, or 1,000 Gigabytes, is the equivalent of 500,000,000 double-spaces pages of text. Computer hard drives are now capable of storing multiple Terabytes of data and are commonplace in new desktop computers. And, this data may be stored in a variety of formats or encrypted. The sheer volume of data also has extended the time that it takes to analyze data in a laboratory. Running keyword searches takes longer and results in more hits that must be individually examined for relevance. Even perusing file structures can be laborious if the user is well-organized. Producing only a directory listing of a home computer can result in thousands of pages of printed material most of which likely will be of limited probative value

5. Based on the foregoing, searching any computer or forensic image for the information subject to seizure pursuant

RSB 2/24/2016

to this warrant may require a range of data analysis techniques, and may take weeks or even months. Keywords need to be modified continuously based upon the results obtained. Evidence in graphic file format must be laboriously reviewed by examiners. Criminals can mislabel and hide files and directories, use codes to avoid using keywords, encrypt files, deliberately misspell certain words, delete files, and take other steps to defeat law enforcement.

6. ***Persistence of Digital Evidence***. Computers store data, both on removable media (for example, CDs and floppy diskettes) and internal media, in ways that are not completely known or controlled by most users. Once stored, data is usually not destroyed until it is overwritten. For example, data that is "deleted" by a user is usually not actually deleted until it is overwritten by machine processes (rather than user decision) that decide where to store data and when overwriting will occur. Therefore, files and fragments of files and other data may easily last months, if not years, if the storage media is retained.

7. Typically, computer forensics focuses on at least three categories of data. These are: 1) active data - such as current files on the computer, still visible in file directories and available to the software applications loaded on the

2/26/2016

computer; 2) latent data – such as deleted files and other data that resides on a computer's hard drive and other electronic media in areas available for data storage, but which are usually inaccessible without the use of specialized forensic tools and techniques; and 3) archival data – such as data which has been transferred or backed up to other media such as CDs, floppy disks, tapes, and ZIP disks.

8. Active data includes not only files created by and with the user's knowledge, but also may include items such as Internet history log files, system registry files (listing all the systems and software applications installed on a computer, including the dates of installation, use, and deletion), and date/time file stamps automatically created that identify when files were created, modified, and last accessed.

9. Latent data includes data retained and stored on computer media in "unallocated" and "slack" space. Unallocated space refers to space on a hard drive that is available for the storage of new data. Slack space refers to any leftover space that remains when an active file is stored in particular location on the hard drive that is akin to an empty shelf in a closet containing other full shelves. Deleted files and other latent data that has not been overwritten by new data or files often may be accessed by a qualified forensic examiner from the

RSB 2/26/2016

unallocated and slack space on a computer user's hard drive months and years after such data was created by the user or the computer's operating system.

10. I know, based upon my training and experience, that a qualified forensic examiner may use knowledge of the mechanisms used to store electronic data to unlock and to uncover the activities of a computer's user years after the fact by examination of active, latent, and archival data. Through the use of proper computer forensic techniques such data and evidence of criminal offenses may be recovered, notwithstanding the passage of time since a crime occurred.

11. In light of these difficulties, I request permission for investigators to remove to a forensically-secure location the computers or cell phones and computer-related equipment as instrumentality(ies) of the crimes, and to use whatever data analysis techniques reasonably appear necessary to locate and retrieve digital evidence within the scope of this warrant. Such action will greatly diminish the intrusion of law enforcement into the premises and will ensure that evidence can be searched for without the risk of losing, destroying or missing the information/data for which there has been authorization to search.

RSB 2/26/2016

Conclusion

Based upon the foregoing, I submit that there is probable cause to believe that the property described in Attachment A, contains evidence, contraband, fruits and instrumentalities pertaining to violations 18 U.S.C. § 875 (C) (Interstate Communication), 871 (Threats to the President), 879 (Threats to Former President's) among other possible federal offenses. I therefore respectfully request that the attached search warrant be issued authorizing the search of property described in Attachment B.

Thomas W. Fleming
Senior Resident Agent
US Secret Service

Subscribed and sworn
before me this 26th of February, 2016

Robert S. Ballou
United States Magistrate Judge

ATTACHMENT A
PROPERTY TO BE SEARCHED

HP PAVILION LAPTOP COMPUTER, SN 5CD3367NVV6

2/26/2016

ATTACHMENT B

Property to be seized

1. All records and objects relating to violations of Title 18 USC § 875 (C), 871, or 879 including:

a. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. Evidence of internet research of government officials; locations of government buildings; weapons research or purchase information for weapons of any kind; review of any computer maps program and the search history of any such program; any photo file which may contain the photos of persons searched or any photo which may show the travel history of Karsten SHEPHERD;

c. Evidence of the use of LinkedIn, including creating or editing the profile, sending

communications from LinkedIn, and sending threats of any kind whether by LinkedIn, email, or any other electronic or social media platform;

d. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

e. Evidence of the lack of such malicious software;

f. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. Evidence of the times the COMPUTER was used;

i. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. Records of or information about Internet Protocol addresses used by the COMPUTER;

l. Records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2/26/2016